REMARKS

Claim rejections under 35 USC 101

Claims 1, 3-8, and 10-18 have been rejected under 35 USC 101 because the Examiner believes that the claims disclose an invention that is inoperative and thus lacks utility. In particular, the Examiner states that the invention is directed towards secure communication involving keys, but that the claim limitations prohibit all processes from accessing the keys. Applicant has amended the claims so that it is clear that just all the *user* processes cannot access the keys. For instance, *kernel* processes (i.e., kernel *agents*) have access to the keys. Applicant has provided a reference, "Kernel Extensions and Device Support Programming Concepts" with this response that disclose the distinction between kernel and user processes. As a result of this amendment, Applicant submits that the claims satisfy 35 USC 101, in that they are indeed operable.

Claim rejections under 35 USC 112

Claims 1, 3-8, and 1-18 have been rejected under 35 USC 112, first paragraph, as failing to complying with the written description requirement, and under 35 USC 112, second paragraph, as being indefinite. The crux of both of these rejections is that the keys are inaccessible by all processes. As stated above in relation to 35 USC 101, the claims have been amended so that it is clear that the keys are inaccessible by all *user* processes, such that, for instance, *kernel* processes (i.e., kernel *agents*) have access to the keys. As a result of this amendment, Applicant submits that the claims satisfy 35 USC 112, first and second paragraphs.

Claim rejections under 35 USC 103(a)

Claims 1, 3-7, 11, and 14-16 have been rejected under 35 USC 103(a) as to Stein ("Web Security . . .", 1998, ISBN 0201634899) in view of Carter (5,845,331). Claims 1, 3-7, 11, and 14-16 have been rejected under 35 USC 103(a) as to Stein in view of Fontana ("Web Security . . . ", 2000, http://www.networkworld.com). Claim 8 has been rejected under 35 USC 103(a) as to Stein in view of Carter and further in view of Ogawa (5,802,065). Claim 16 has been rejected under 35 USC 103(a) as being unpatentable over Stein view of Carter and further in view of Baker. Claims 12-13 and 17-18 have been rejected under 35 USC 103(a) as being unpatentable over Stein in view of Carter, Baker, and Ogawa, and further in view of Bean (4,843,541). Claims 12-13 and 17-18 have been rejected under 35 USC 103(a) as being unpatentable over Stein in view of Fontana. Claims 1 and 10 have been rejected under 35 USC 103(a) as to Win (6,161,139) in view of Fontana.

Applicant notes that claims 1, 11, and 15 are independent claims, from which the remaining pending claims depend. Applicant asserts that claims 1, 11, and 15 are patentable, such that the remaining pending claims are patentable for at least the same reasons. Applicant specifically discusses claim 1 as representative of independent claims 1, 11, and 15 insofar as patentability over Stein in view of Carter is concerned.

Claim 1 is limited to a key sent by hardware of a first node that is accessible only by a kernel agent of the first node, to hardware of a second node that is accessible only by a kernel agent of the second node. The key is thus inaccessible by all user processes running on the first and second nodes. Applicant refers the Examiner to the cofiled reference "Kernel Extensions and Device Support Programming Concepts" for information as to the distinction between user processes and kernel processes (i.e., kernel agents). Secure communication is therefore achieved in the claimed invention because the user processes have no access to the keys, only the kernel processes have access to the hardware that stores these keys.

By comparison, Stein in view of Carter or Fontana and Win in view of Fontana are silent as to the distinction between kernel and user processes, and indeed do not provide for user processes not having access to the keys. In fact, Stein in view of Carter or Fontana and Win in view of Fontana disclose user processes that have access to keys. For instance, Stein notes that "[t]he *browser* encrypts the [premaster] secret using the server's RS public key" in paragraph 6 on page 42. A browser is a user process, as can be appreciated by those of ordinary skill within the art (i.e., it is definitely not a kernel process, as is also readily understood by those of ordinary skill within the art) and thus has access to the secret that the Examiner identifies as the key sent from the first node to the second node, inherently while it is encrypting the secret. Although it should be readily evident that a browser is a user process and not a kernel process, see also page four of the "Application Architecture" reference that has been provided with this response, in which it is said that a "client can be a Web browser or other end-user process." (P. 4) Furthermore, as to Win, as stated by the Examiner, Win teaches sending a key (specifically a cookie) to a client web browser. As has been stated, however, a browser is a user process, and not a kernel process, and thus the client web browser has access to the key. By comparison, the claimed invention is limited to *all user* processes – including user processes such as browsers – not being able to access the key.

It is noted that the primary prior art references cited by the Examiner as to the independent claims in rejecting these claims – Stein and Win – have to do with web browsing. Those of ordinary skill within the art can appreciate that web browsing processes are user processes, and not kernel processes, as is further evidenced by the "Application Architecture" reference noted above. In some instances, you could have a user process run in kernel mode, but it is still a user process running in kernel mode, and not a kernel process. See, for instance, the "Kernel Mode Linux" reference that has been provided in this response, which discloses that "user programs can be executed *as user processes* that have the privilege level of kernel mode." Running user processes like browsers in kernel mode therefore still does not disclose claim 1,

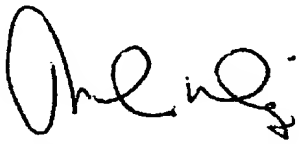
because claim 1 is limited to all user processes being unable to access hardware that is accessibly only by kernel agents. That is, if user processes like browsers run in kernel mode, then they are able to access the hardware of claim 1, whereas claim 1 is limited to user processes not being able to access this hardware.

Therefore, Stein in view of Carter or Fontana and Win in view of Fontana disclose user processes having key access. By comparison, the claimed invention is limited to user processes not having key access. To this end, Stein in view of Carter or Fontana and Win in view of Fontana do not render the claimed invention unpatentable under 35 USC 103.

Conclusion

Applicants have made a diligent effort to place the pending claims in condition for allowance, and request that they so be allowed. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Applicants' Attorney so that such issues may be resolved as expeditiously as possible. For these reasons, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,



August 31, 2005
Date

Michael A. Dryja, Reg. No. 39,662
Attorney/Agent for Applicant(s)

Law Offices of Michael Dryja
704 228th Ave NE #694
Sammamish, WA 98074
tel: 425-427-5094, fax 206-374-2819